07.29.05

AF RAW 2182

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Eliyahou Harari et al.		
Assignee:	SanDisk Corporation		
Title:	Removable Mother/Daughter Peripheral Card		
Application No.:	10/050,429	Filing Date:	May 15, 2002
Examiner:	Huynh, Kim Ngoc	Group Art Unit:	2182
Docket No.:	SNDK.044US7	Conf. No.:	6805

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF APPEAL BRIEF

Sir:

Pursuant to 37 C.F.R. § 1.191 and the Notice of Appeal filed in this application on June 24, 2005, Applicants submit this Appeal Brief. In accordance with 37 C.F.R. § 41.20(b)(2), a check is enclosed that includes the fee of $500.00 for this Appeal Brief. The Commissioner is also authorized to deduct any other amounts required for this Appeal Brief and to credit any amounts overpaid to Deposit Account No. 502664. This paper is submitted in duplicate to facilitate the appeal procedures and deposit account payment.

EXPRESS MAIL LABEL NO:

EV627931593US

Respectfully submitted,

July 27, 2005
Date

Gerald P. Parsons
Reg. No. 24,486
PARSONS HSUE & DE RUNTZ LLP
655 Montgomery Street, Suite 1800
San Francisco, CA 94111
(415) 318-1160 (main)
(415) 318-1163 (direct)
(415) 693-0194 (fax)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Eliyahou Harari et al.		
Assignee:	SanDisk Corporation		
Title:	Removable Mother/Daughter Peripheral Card		
Application No.:	10/050,429	Filing Date:	May 15, 2002
Examiner:	Huynh, Kim Ngoc	Group Art Unit:	2182
Docket No.:	SNDK.044US7	Conf. No.:	6805

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is being submitted in triplicate in accordance with 37 C.F.R. §41.37 and the Notice of Appeal filed in this application on June 24, 2005.

I. REAL PARTY IN INTEREST

The real party in interest is SanDisk Corporation, as named in the caption above, which is the assignee of the applicants.

II. RELATED APPEALS AND INTERFERENCES

Based on information and belief, there are no appeals or interferences that could directly affect or be directly affected by or have a bearing on the decision by the Board of Patent Appeals in the pending appeal.

III. STATUS OF CLAIMS

Original application claims 1 – 49 have been cancelled.

Claims 50 – 82 remain in the application and have all been finally rejected. This appeal is being taken from the final rejection of all of claims 50 – 82.

IV. STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

There are six independent claims. Independent claims 50, 63 and 66 recite methods of storing and retrieving user data from a non-volatile memory card. Independent claims 67, 71 and 79 define memory cards or a more general data storage system. None of the claims 50 – 82 in the present application contain a means plus function or step plus function limitation within the meaning of 35 U.S.C. § 112, sixth paragraph.

A primary claimed feature is storing encoded user data in the memory along with some information about the data encoding, namely information useful to decode the user data. This is included in each of the independent claims. Examples of data encoding and decoding described in the specification include compressing and decompressing the data, and encrypting and decrypting the data. (See the specification, Summary of the Invention, page 10, lines 3 – 11, and Detailed Description, page 27, lines 3 – 15.) Some of the claims, namely independent claim 79 and dependent claims 51 – 53, 68 – 70, 72, 73, and 80 – 82, specifically recite that the

encoding/decoding includes compression/decompression or encryption/decryption. The type of information about the encoding that is stored in the memory along with the encoded data includes a key or algorithm for recovering the data. (Also in the Summary of the Invention, page 10, lines 3 – 11, and the Detailed Description, page 27, lines 3 – 15.)

This feature allows data encoded and stored on the memory card by one host system to be decoded and read when connected with a separate host system. The information necessary to decode the data is provided to the second host from the same memory. A second claimed feature is this use of memory cards to transfer encoded data between hosts, included in independent method claims 63 (and thus its dependent claims 64 and 65) and 66, and in dependent claims 59 – 61. (Also described in the Summary of the Invention, page 10, lines 3 – 11, and the Detailed Description, page 27, lines 3 – 15.)

A third claimed feature is implementation of the memory system in two cards, one (a daughter card) containing memory without a controller therefore, and another (a mother card) containing the memory controller. The daughter card connects with the mother card, and the mother card connects with the host. Claims 61, 63, 64 and 66 recite that the encoding or decoding, or both, of the data stored in the memory card is performed by the controller in the mother card. (See the specification, page 17, line 28 through page 18, line 2, with respect to Figure 5B, and page 25, line 14 through page 27, line 2, with respect to Figure 9.) The optional functional components 42 of the mother card 10 encode and/or decode the data.

Each of the three claimed features summarized above is separately discussed in the Argument below. It should be noted that claims 61 and 63 – 66 contain limitations to all three of the features identified above.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) The rejection of claims 50 – 63 and 66 – 82 under 35 U.S.C. § 102(b) as being anticipated by U.S. patent no. 5,357,573 ("Walters");

2) The rejection of claims 50 – 64 and 66 – 82 under 35 U.S.C. § 102(b) as being anticipated by U.S. patent no. 5,093,731 ("Watanabe et al.");

3) The rejection of claims 50 – 63, 66 – 70 and 79 – 81 under 35 U.S.C. § 102(b) as being anticipated by U.S. patent no. 4,935,962 ("Austin");

4) The rejection of claims 50 – 63, 66 – 70 and 79 – 81 under 35 U.S.C. § 102(b) as being anticipated by U.S. patent no. 4,656,474 ("Mollier et al.");

5) The rejection of claims 50 – 63, 66 – 70 and 79 – 81 under 35 U.S.C. § 102(b) as being anticipated by U.S. patent no. 4,816,651 ("Ishording");

6) The rejection of claims 50 – 63, 66 – 70 and 79 – 81 under 35 U.S.C. § 102(b) as being anticipated by U.S. patent no. 5,343,530 ("Viricel"); and

7) The rejection of claim 65 under 35 U.S.C. § 103(a) as being obvious over the Watanabe et al. patent alone.

VII. ARGUMENT

A. The Statutory Basis of the Anticipation Rejections over the Walters and Viricel Patents Is in Incorrect

Since the Walters and Viricel patents were granted after the effective filing date of the present continuation application, they cannot be used to form a rejection under 35 U.S.C. § 102(b). There is no other evidence of record that they or their contents were published more than one year prior to the latest possible effective filing date of November 12, 1993, to which the present application is entitled.

The present application is a continuation claiming priority from an initial parent application filed September 1, 1993, and a continuation-in-part of that application filed November 12, 1993. The present claims, therefore, have an effective filing date of at least as early as November 12, 1993. Since the Walters patent was granted on October 18, 1994, and the Viricel patent on August 30, 1994, both after the effective filing date of the present application, they are not bars to patentability under 35 U.S.C. § 102(b).

B. None of the Six Cited References Anticipate the Feature of Storing Encoded User Data in the Memory Along with Some Information About the Data Encoding, Namely Information Useful to Decode the User Data, as Recited in All the Claims 50 – 82.

Each of the independent method claims 50, 63 and 66 specify that user data are encoded and stored in the non-volatile memory card along with information useful to decode the stored encoded data. The encoded data and information are then read from the memory card and the

information read from the memory card is used to decode the data. A different host from the one that originally encoded and stored the data can then be used to decode the data, as further expressed in claims 63 and 66.

Similarly, the independent memory card and data storage system claims 67 and 79 specify that both encoded data ("encrypted data" in claim 79) and information useful to decode these data are stored in the memory. Independent claim 71 is somewhat different in reciting a memory card that has a built-in data encoder and decoder. Data received from a host is then encoded by the card and the encoded data stored in its memory. When the data are read by a connected host, they are decoded by the built-in decoder. The card encoder/decoder permanently contains information of the encoding of data stored on the card.

It is submitted that none of the six cited patents anticipate this feature as it is claimed. The rejections under each of the six cited patents are discussed separately.

U.S. patent no. 5,357,573 ("Walters")

In Walters, a software program is stored in a memory card along with a protection routine and a comparison code that protect the software program from unauthorized use. The protection routine is run when the software program is accessed through a host to which the memory card is connected. The protection routine compares its comparison code with a protection code stored in the card, either in a separate read-only-memory (ROM) or as part of the main static-random-access-memory (SRAM) or dynamic-random-access-memory (DRAM) that stores the software program. If they compare, the software program is allowed to run on the host; if they do not compare, the protection routine prevents the software program from running on the host. The protection routine and code operate to control access to the software program, not to decode the software program.

Although the protection and comparison codes may be encrypted, no suggestion has been found in the Walters patent of encoding the protected software program. It seems clear that the software program is stored in the memory card without any encoding. Indeed, the Walters patent teaches away from encoding the software program since an advantage of its technique is stated to be that the software program may be executed directly from the memory card without having to

be loaded into the memory of the host (col. 4, lns. 27-30), something that would be more difficult if some form of real time decoding of stored encoded data was required.

The final Office Action (page 2, para. a) contends that the protection routine and code are "useful information for encoding/decoding process." This is believed to be in error since the protected software code is not encoded by the protection routine and code. Rather, the protection routine and code simply provide control of access to the software program stored in the card.

In a response to arguments presented against this same rejection made in the first non-final Office Action, the final Office Action (page 6, lines 2-3) states that "Walter discloses the application program is modified by the protection code and both are stored in the memory card." This is submitted to be incorrect. The software program is modified to work with the protection routine but the protection routine only utilizes the protection code to prevent unauthorized use of the software program stored on the memory card. The software program is not encoded by the protection code.

There is also one other point of novelty in the claims over the Walters patent. Although the ROM within the memory of Walters that stores the protection code may be a flash memory chip (which is then disabled from altering the protection code), the main memory is disclosed by Walters to be either SRAM or DRAM (col. 3, ln. 62 – col. 4., ln. 2). All of the claims, on the other hand, call for encoded data to be stored in a non-volatile memory. Further, independent claim 67 and dependent claims 57 and 58 specify flash memory. The final Office Action did not respond to this point that was made earlier.

U.S. Patent No. 5,093,731 ("Watanabe et al.")

The Watanabe et al. patent does describe use of a memory card 1 with a camera 10 (dependent claim 64 defines the host to be a camera) but, it is respectfully submitted, does not suggest the fundamental limitations of the claims. Nothing has been found in Watanabe et al. about storing its picture data in an encoded form, and there is therefore nothing about storing "information useful to decode" such data in the memory card. Since both of these limitations are part of each of the each of the rejected claims 50 – 70, the Watanabe et al. patent cannot be held anticipate them.

The final Office Action (page 6, lines 3-5) in a response to these arguments previously presented, states that "Watanabe discloses a compression/decompression algorithm for storing the image data and the image data stored in the memory card." However, no such compression or decompression has been found to be disclosed. A scan of the text of the Watanabe patent on the USPTO web site found no instances of use of any form of the words "compress" or "decompress." Besides, even if this quoted response is correct, it does not establish anticipation of the claim feature being discussed, namely the storage in a memory of both encoded data and information useful to decode the data.

There are two items of information described by Watanabe et al. to be stored along with the picture data. The data of one picture and this other information are stored in an individual one of the memories 2. One item of information is a "recording sequence code" which is simply a sequential number from the camera of the picture stored in the memory. The second item of information is a "recording-finished code" which is "data indicating whether a recording has been made" (Watanabe et al., col. 3, lns. 54-55); that is, in the nature of a flag indicating whether there is picture data stored in the one of the memories 2 in which the code is stored. So even if the picture data stored in the memory card are somehow argued to be encoded, even though not described in Watanabe et al. to be encoded, there is no information stored along with the picture data that is "useful to decode" (claim 50) the picture data.

It may be noted that the Watanabe et al. patent is the only reference upon which dependent claim 64 is rejected as being anticipated. It is also the only reference used in the rejection of dependent claim 65, on obviousness grounds.

U.S. Patent no. 4,935,962 ("Austin")

Austin's first embodiment, upon which the Office Action seems to rely, is a technique of authenticating the card 30 (Figure 2). The issuer of the card 30 calculates a series of values S_1 . . S_n from a public value N and a secret key d, and then stores the values S_1 . . S_n in the secure memory 42, along with the public value N. (Col. 5, ln. 58 – col. 6, ln 12.) To authenticate the card, the card acceptor device 32, to which the memory card 30 is connected, generates a random number v and sends it to the card. The card then calculates Y from v, N and S_1 . . S_n, and sends Y to the acceptor device 32. The acceptor device 32 then makes a calculation from the public

values F_1 . . F_n, N and v, and makes a further calculation from the value Y received from the card. By comparing two values resulting from the calculations, the acceptor device 32 then determines whether the card is authentic (col. 8, ln. 40 – col. 7, ln. 13).

It is not understood how this could possibly anticipate the present application claims. No data are described to be stored in the memory card, with which the rejected claims are directed. None of the card authenticating values N and S_1 . . S_n that are stored on the memory card 30 are said to be encrypted. Indeed, the only portion of the Austin patent referenced in the Office Action to discuss data encoding or decoding is a Background discussion (col. 1, ln. 61 – col. 2, ln. 8) of public key cryptography, after which it is dismissed by Austin as ". . not practical for low cost replicated entities." (col. 2, lns. 28-29.) An improvement then described by Austin is much different and does not involve storing encoded data on the memory card.

A second embodiment described with respect to Figure 4 of the Austin patent (begins at col. 7, ln. 51) stores a message M on a memory card 30A that is authenticated by appending an authentication code (certificate) to the message. Neither the message M or the authentication code appear to be encoded in any manner.

The memory cards described in the Austin patent appear to be designed to give access of an individual to an electronic system. This access is granted only after the authenticity of the card is verified. This is quite different from the present application claims where data are stored on a memory card in an encoded way, along with information on how to decode the data.

U.S. Patent No. 4,656,474 ("Mollier et al.")

The Mollier et al. patent describes a technique of authenticating the signature of a signed message that has been received. The signature is attached to the message to authenticate it but no mention of encrypting the message has been found. This is confirmed by the three passages of the Mollier et al. patent referenced in the final Office Action. Parameters stored in memory along with data of the message M are used by the sender to form an identification I which is characteristic of the sender. The identification I is joined with the message M and sent.

It seems clear that the Mollier et al. patent does not suggest storing user data in an encoded form along with information useful to decode it, as defined by the rejected claims. It is submitted that the final Office Action (page 4, lns. 10-17) is in error in stating that the Mollier et

al. patent discloses storing message data M in an encoded form and uses information stored with it to decode the message data. Rather, the portions of the Mollier et al. patent specifically cited in the Office Action discuss sending the message M with an identification I that authenticates the message, not that provides the recipient information necessary to decode the message M. No mention of the message M being encoded has been found in the Mollier et al. patent.

U.S. Patent No. 4,816,651 ("Ishording")

Similarly, no suggestion has been found in the cited Ishording patent of storing its data INF in an encoded form in a memory card (on the right of Figure 1) along with information useful to decode the data, as claimed. Rather, the data INF are encoded in the course of a processing device (on the left of Figure 1) reading the data INF from the memory card. As shown in Figure 2 for reading data from the memory card, the data INF are encoded by a number X randomly generated in the processing device and sent to the memory card after being encoded with a key SK stored in both the memory card and processing device. The encoded data are then decoded in the processing device by use of the random number X that it generated. The claimed idea of storing encoded data along with information useful to decode the data is not present. The data INF are not described in the Ishording patent to be stored in an encoded form in the memory card but rather are encoded with a number generated by the processing device only when the data INF are read from the memory card.

U.S. Patent No. 5,343,530 ("Viricel")

We must similarly respectfully disagree that the Viricel patent "discloses a system for storing both encoded data D and information [key K and algorithm C] useful to the decoding of the data", as alleged in the final Office Action (page 5, lns. 1-3). Although an encryption program is stored in the ROM 14 of the memory card 10, no mention has been found that data are stored in the memory card in an encrypted form. Rather, stored data are used along with other parameters to generate an encrypted quantity within the card that is compared with a similar quantity calculated by an attached transaction instrument. The purpose of Viricel is to authenticate the card, not to store and transfer data from the card.

C. None Of the Six Cited References Anticipate the Method Of One Host Encoding and Storing the Encoded Data on The Memory Card and a Second Host Decoding and Reading the Data from the Card, as Recited in Claims 59 – 61 and 63 – 66.

Independent method claims 63 and 66 additionally recite that the above-discussed method is implemented by connecting the memory card with a first host that stores data on the card and then connecting the memory card with a second host that reads the data from the card. The data are encoded at the first host and stored on the card along with information useful to decode the user data. The second host reads the decoding information and the encoded data from the card, and decodes the data by use of the decoding information. The second computer is able to decode the stored data because information useful to decode the data is also stored on the memory card. Dependent claim 59 introduces the came concept.

The only mention in the final Office Action of this feature is a reference (paragraph bridging pages 2 and 3) to the Walters patent as disclosing first and second computers to which a memory card is connected. However, it is not understood how the Walters patent describes the memory card "connected to the first computer system (hence the mother board) during the production and second host during usage of the memory," or if it does, how this would anticipate any of the claims. A previous argument made in response to this rejection in the first Office Action was not answered but rather the ground of rejection was merely repeated in the final Office Action without any further comment.

None of the six cited references are seen to suggest the two host usage specified in claims 59 – 61 and 63 – 66.

D. None of the Six Cited References Anticipate the Feature of Forming the Memory System with Two Cards, One (Daughter Card) Containing Memory Without a Controller Therefore, and Another (Mother Card) Containing the Controller that Performs Encoding and Decoding, as Recited in Claims 61, 63, 64 and 66.

Rejected independent method claims 63 (and thus also its dependent claim 64) and 66, and claim 61 that is dependent through claim 59 on claim 50, additionally specify a particular use of both a memory (daughter) card and a mother card that contains the controller for the

memory. The memory card is connected to a host either through the mother card, when the host does not carry out the memory controller function, or directly to the host, when it does.

In independent claim 63, data are encoded and stored on the memory card along with the decoding information by a first host to which the memory card is directly connected. These data are then read and decoded by the controller function of the mother card that is connected with a second host and with which the memory card is connected. Independent claim 66 recites a similar method but where the mother card is used to encode and store data on the card from a first host and the second host accepts the memory card directly and decodes the data with its internal controller. Claim 66 recites a method that is in effect the inverse of the method of claim 63.

The Office Action (paragraph bridging pages 2 and 3) takes the position that a computer motherboard is inherent in the Walters patent and is the claimed mother card. Further, it is said to be inherent that the memory card would be moved between hosts during production and use. When the memory card is plugged into one such computer, it is apparently being asserted that its motherboard is the claimed mother card. But when the memory card is plugged directly into the second computer, according to the claims, no mother card is being used. So the motherboard of the second computer, since motherboards are alleged to be the claimed mother cards, would therefore not be used. Since the memory card would likely not work with a second computer without its motherboard, it is not seen how the methods of claims 61, 63, 64 and 66 could possibly be considered to be inherent from the Walters patent.

The speciousness of this ground of rejection becomes apparent when it is noted that the Walters patent does not even mention a computer motherboard, let alone provide any basis for concluding that such a motherboard is used in the manner claimed. The Walters patent is directed to a memory card. A computer is only mentioned, not shown, as something with which the card is used. It was previously argued by the undersigned attorney that such a disclosure is not inherent in the Walters patent and that the Office Action is taking Official Notice of subject matter not disclosed in the cited prior art. In response to this argument, the final Office Action contains a strong response (page 6, line 12 through page 7, line 7), with reference to three undated new references found on the Internet. These undated Internet references were not applied against any claims in the final Office Action.

There is no dispute that personal and other types of computers contain motherboards. What is in dispute is whether the detailed methods of claims 61, 63, 64 and 66 are inherent in the Walters patent just because the computer it mentions is likely to contain a motherboard. The claimed methods involve moving a memory card from one host to another, one host operating with the assistance of a mother card that is connected to it and the other not. It is submitted that this ground of rejection is in error.

Although claims 61, 63, 64 and 66 have also been rejected as anticipated by the other five cited references (Watanabe et al., Austin, Mollier et al., Ishording and Viricel), the final Office Action does not identify any disclosure relating to the mother/daughter card feature of these claims. Indeed, none can be found.

E. Claim 65 Would Not Have Been Obvious Over the Watanabe Reference

Claim 65 has not been rejected under 35 U.S.C. § 102(b), as are the remaining claims, but rather only under 35 U.S.C. § 103(a) over the Watanabe et al. patent alone. Claim 65 is submitted to be patentable for the same reasons discussed above that render its independent parent claim 63 novel over the Watanabe et al. patent. Claims 63 and 65 describe a detailed method of using a memory card with two hosts wherein a mother card is also employed. Nothing like this is suggested in the Watanabe et al. patent or in any of the other five cited patents. Indeed, claims 63 and 65 each include all three of the novel features discussed above. Claim 65 is therefore certainly patentable.

F. Conclusion

For the reasons stated above, it is submitted that:

1) Each of claims 50 – 82 is not anticipated by any of the six references cited against it because of the feature of storing encoded user data in the memory along with some information about the data encoding, namely information useful to decode the user data;

2) Each of claims 59 – 61 and 63 – 66 is not anticipated by any of the six references cited against it because of the feature of one host storing encoded data on the memory card along with information allowing the data to be decoded, and then another host decoding the data using such stored information;

3) Each of claims 61, 63, 64 and 66 is not anticipated by any of the six references cited against it because of the feature of forming the memory system with two cards, one (mother card) containing a memory controller that encodes and decodes the data, to which another (daughter card) containing memory is connectable; and

4) Claim 65 would not have been obvious over the Watanabe et al. patent, one of the six cited patents.

The final rejection should thus be overturned and all of the claims 50 – 82 allowed.

EXPRESS MAIL LABEL NO:

EV627931593US

Respectfully submitted,

Gerald P. Parsons — July 27, 2005

Gerald P. Parsons
Date
Reg. No. 24,486

PARSONS HSUE & DE RUNTZ LLP
655 Montgomery Street, Suite 1800
San Francisco, CA 94111
(415) 318-1160 (main)
(415) 318-1163 (direct)
(415) 693-0194 (fax)

VIII. CLAIMS APPENDIX

50. A method of storing user data on and retrieving user data from a non-volatile memory card, comprising:

encoding the user data,

storing both the encoded user data and information useful to decode the encoded user data on the memory card,

thereafter reading both the encoded user data and the decoding information from the memory card, and

decoding the read encoded user data by use of the decoding information read from the memory card, thereby to obtain the user data.

51. The method of claim 50, wherein encoding the user data includes compressing the user data, and the decoding information stored on the memory card includes a decompression algorithm.

52. The method of claim 50, wherein encoding the user data includes encrypting the user data, and the decoding information stored on the memory card includes a decryption algorithm.

53. The method of claim 50, wherein encoding the user data includes encrypting the user data, and the decoding information stored on the memory card includes a decompression key.

54. The method of claim 50, wherein the decoding information includes an algorithm useful to decode the encoded user data.

55. The method of claim 50, wherein the decoding information includes an key useful to decode the encoded user data.

56. The method of claim 50, wherein the decoding information includes a software or hardware driver useful to decode the encoded user data.

57. The method of claim 50, wherein the non-volatile memory card includes a flash EEPROM array, and both the encoded user data and the decoding information are stored in the flash EEPROM array.

58. The method of claim 57, wherein storing includes programming both the encoded user data and decoding information into individual memory cells of the flash EEPROM array in more than two states, thereby to store more than one bit of said user data and decoding information per cell.

59. The method of claim 50, wherein the encoding and storing occur when the memory card is electrically connected to a first host system, and wherein the reading and decoding occur when the memory card is electrically connected to a second host system.

60. The method of claim 59, wherein either the encoding is accomplished by the first host system or the decoding is accomplished by the second host system.

61. The method of claim 59, wherein at least one of the encoding and decoding are accomplished in a memory controller function included in a mother electronic card that is removably connectable with at least one of the first and second host systems and into which the memory card is removably connectable.

62. The method of claim 50, wherein at least one of the encoding and decoding are accomplished in a memory controller function included in a mother electronic card to which the memory card is removably connectable.

63. A method of storing user data on and retrieving user data from a non-volatile memory card, comprising:

connecting the memory card to a first host system,

encoding the user data within the first host system,

storing the encoded user data and information useful to decode the user data on the memory card from the first host system,

removing the memory card from connection with the first host system,

connecting a mother card to a second host system, wherein the mother card includes a controller function for the memory card,

connecting the memory card to the mother card,

thereafter causing the mother card to read the encoded user data and the decoding information from the memory card, and

decoding the read encoded user data within the controller function of the mother card by use of the decoding information read from the memory card, thereby to provide the user data to the second host.

64. The method according to claim 63, wherein the first host system includes a camera and the user data includes visual field data obtained by the camera.

65. The method according to claim 64, wherein the second host system includes a personal computer.

66. A method of storing user data on and retrieving user data from a non-volatile memory card, comprising:

connecting a mother card to a first host system, wherein the mother card includes a controller function for the memory card,

connecting the memory card to the mother card,

encoding user data provided by the first host system within the mother card controller function,

storing on the memory card the encoded user data and information useful to decode the user data,

removing the memory card from connection with the mother card,

thereafter connecting the memory card to a second host system without use of the mother card,

thereafter causing the second host system to read the encoded user data and the decoding information from the memory card, and

decoding the read encoded user data with the second host by use of the decoding information read from the memory card, thereby to obtain the user data.

67. A non-volatile memory card, comprising:

a flash EEPROM array,

encoded user data stored in a first portion of the array, and

data of information useful to decode the encoded user data stored in a second portion of the array.

68. The memory card of claim 67, wherein the stored encoded user data includes compressed user data, and wherein the information useful to decode the stored encoded user data includes a decompression algorithm.

69. The memory card of claim 67, wherein the stored encoded user data includes encrypted user data, and wherein the information useful to decode the stored encoded user data includes a decryption algorithm.

70. The memory card of claim 67, wherein the stored encoded user data includes encrypted user data, and wherein the information useful to decode the stored encoded user data includes a decryption key.

71. A memory system card, comprising:

a connector adapted to be received by a host system,

a receptacle adapted to receive a memory card that includes non-volatile memory,

a controller for programming data into and reading data from the non-volatile memory in response to commands from a host system,

an encoder of data received from a host system, thereby causing encoded data to be stored in the non-volatile memory, and

a decoder of encoded data read from the non-volatile memory, thereby causing decoded data to be provided to a host system.

72. The memory system card of claim 71, wherein the encoder functions to compress the data received from a host system, and the decoder functions to decompress the encoded data read from the non-volatile memory.

73. The memory system card of claim 71, wherein the encoder functions to encrypt the data received from a host system, and the decoder functions to decrypt the encoded data read from the non-volatile memory.

74. The memory system card of claim 71, wherein the decoder operates with information of a decoding algorithm read from a memory card connected with the system card receptacle.

75. The memory system card of claim 71, wherein the decoder operates with a key read from a memory card connected with the system card receptacle.

76. The memory system card of claim 71, wherein the decoder operates to decode encoded data read from the non-volatile memory by use of information also stored in the non-volatile memory about the data encoding.

77. The memory system card of claim 76, wherein the information includes a data decoding algorithm.

78. The memory system card of claim 76, wherein the information includes a decoding key.

79. A data storage system, comprising:

a re-programmable non-volatile semiconductor memory,

first data encrypted and stored in the memory,

second data stored in the memory of information useful to decrypt the first data,

a controller operably connected with the memory to decrypt the first data by use of the second data, and

a connector electrically connected with the controller in a manner to pass the decrypted first data therethrough and adapted for removable connection with different host devices.

80. The data storage system of claim 79, wherein the information useful to decrypt the first data includes a decryption algorithm.

81. The data storage system of claim 79, wherein the information useful to decrypt the first data includes a decryption key.

82. The data storage system of claim 79, formed in first and second cards that are removeably connectable with each other through mating connectors, wherein the memory having the first and second data stored therein is located on the first card, and wherein the controller and host connector are located on the second card.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None